CLAIMS

We claim:

1. A method of providing a mobile computing machine with privileged access to a computing resource, the method comprising the steps of:

obtaining a certificate with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;

providing the certificate to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource; and

establishing access to the computing resource using authorization information obtained from the authenticator, the authorization information corresponding to the authenticated identity of the mobile computing unit.

2. The method of claim 1 wherein the mobile computing unit communicates with the computing resource using at least one wireless link.

3. The method of claim 1 wherein the authorization information includes a key for encrypting communications from the mobile computing unit to an input port.

4. The method of claim 3 wherein the key is a symmetric session key.

5. The method of claim 1 further comprising the steps of detecting a failure of a user of the mobile computing unit to complete a logon to access the computing resource and in response performing the step of obtaining a certificate.

6. The method of claim 1 further comprising determining that the mobile computing unit does not have a certificate to prove machine identity and in response performing the obtaining step.

7. The method of claim 1further comprising the step of storing the unique machine identifier on the mobile computing unit for subsequent use.

8. The method of claim 1 further comprising the step of storing the certificate on the mobile computing unit.

9. The method of claim 1 further comprising the step of receiving the unique machine identifier.

10. The method of claim 1 further comprising the steps of obtaining by the domain controller the certificate from a certificate authority; and receiving the certificate from a domain controller.

11. The method of claim 10 wherein the certificate is obtained by the domain controller in response to a user request from a user, the user using the mobile computing unit to access the computing resource.

12. A method of providing a user with privileged access to a computing resource wherein access to the computing resource is restricted, the method comprising the steps of:

requesting access to the computing resource,;

providing a default user identifier to initiate a logon to obtain limited access to the computing resource;

receiving, by an administrator, a default user identifier and in response providing information to obtain access to the computing resource; and

sending and receiving data to and from the computing resource to complete the logon.

13. The method of claim 12 further comprising the step of receiving access to the computing resource conditional on successfully logging into a domain controller, the domain controller corresponding to the computing resource.

14. The method of claim 12 further comprising the steps of obtaining, by the domain controller, a certificate for authenticating the user and receiving, by the user the certificate for authenticating the user from the domain controller.

15. The method of claim 12 wherein the user accesses the computing resource using at least one wireless link.

16. A method of providing a user secure access to a computing resource from an external site, the method comprising the steps of:

sending a request to access a computing resource;

providing a user identifier, the user identifier corresponding to an asserted identity, to a proxy authenticating server via a remote access point;

providing, in response to a challenge, a certificate to authenticate the asserted identity, to the proxy authenticating server via the remote access point; and

receiving an address for sending and receiving data to and from the computing resource, the address corresponding to limited access to the computing resource.

17. The method of claim 16 wherein the address for sending and receiving data is a universal resource locator.

18. The method of claim 17 further comprising receiving by the user a key for encrypting communications to the computing resource.

19. The method of claim 18 further comprising using the key to decrypt communications from the computing resource.

20. A method for setting up a secure link between a server and a client using wireless transmission, wherein the client machine is a wireless station and the server is an authenticator, the client and server securely exchanging keys to establish the secure link with encryption of at least one message exchanged between the client and the server, the method comprising the steps of:

asserting an identity;

responding to an authentication request by providing a certificate to prove the asserted identity; and

generating an initial encryption key for encrypting communications over the secure link from the information in the certificate.

21. A computer-readable medium having computer executable instructions for performing the steps of a method of providing a machine with privileged access to a computing resource, the method comprising the steps of:

obtaining a certificate with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;

providing the certificate to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource; and

establishing access to the computing resource using authorization information obtained from the authenticator, the authorization information corresponding to the authenticated identity of the mobile computing unit.

22. A computer-readable medium as in claim 21, having computer executable instructions for performing the step of using the machine identity is conditional on the failure of a user on the machine to complete a log-in to access the computing resource.

23. A computer-readable medium as in claim 21 having computer executable instructions wherein the mobile computing unit communicates with the computing resource using at least one wireless link.

24. A computer-readable medium as in claim 21 having computer executable instructions wherein the authorization information includes a key for encrypting communications from the mobile computing unit to an input port.

25. A computer-readable medium as in claim 21, having computer executable instructions for performing the additional step of storing the unique machine identifier on the mobile computing unit for subsequent use.

26. A computer-readable medium as in claim 21, having computer executable instructions for performing the additional step of storing the certificate on the mobile computing unit.

27. A computer-readable medium as in claim 21, having computer executable instructions for performing the additional steps of obtaining, by the domain controller, the certificate from a certificate authority; and receiving the certificate from the domain controller.

28. A computer-readable medium as in claim 27 having computer executable instructions wherein the certificate is obtained by the domain controller in response to a user-request from a user to use a computing resource.

29. A computer-readable medium having computer executable instructions for performing the steps of a method of providing a user with privileged access to a computing resource wherein access to the computing resource is restricted, the method comprising the steps of:

requesting access to the computing resource;

providing a default user identifier to initiate a logon to obtain limited access to the computing resource;

receiving, by an administrator, a default user identifier and in response providing information to obtain access to the computing resource; and

sending and receiving data to and from the computing resource to complete the logon.

30. A computer-readable medium as in claim 29, having computer executable instructions for performing the step of receiving access to the computing resource conditional on successfully logging into a domain controller, the domain controller corresponding to the computing resource.

31. A computer-readable medium as in claim 29, having computer executable instructions for performing the steps of obtaining, by the domain controller, a certificate for authenticating the user and receiving, by the user the certificate for authenticating the user from the domain controller.

32. A computer-readable medium as in claim 29 having computer executable instructions wherein the user accesses the computing resource using at least one wireless link.

33. A computer-readable medium having computer executable instructions for performing the steps of a method of providing a user secure access to a computing resource from an external site, the method comprising the steps of:

sending a request to access a computing resource;

providing a user identifier, the user identifier corresponding to an asserted identity, to initiate a log-in in order to access the computing resource;

providing, in response to a challenge, a certificate to authenticate the asserted identity to obtain access to the computing resource; and

receiving an address for sending and receiving data to and from the computing resource.

34. A computer-readable medium as in claim 33 having computer executable instructions wherein the address for sending and receiving data is a universal resource locator.

35. A computer-readable medium as in claim 34 having computer executable instructions for performing the step of receiving a key for encrypting communications to the computing resource.

36. A computer-readable medium as in claim 35 having computer executable instructions for performing the step of using the key to decrypt communications from the computing resource.